OIT-0245-87
5 May 1987

MEMORANDUM FOR: Chief, Information Systems Security Division
Office of Security

VIA: Chief, Management & Consulting Group, OIT

STAT FROM: [redacted]
Acting Chief, Management Division, M&CG
Office of Information Technology

SUBJECT: Security Procedures for Personal Computers

1. The attachment to this memorandum contains our comments on the latest version of the Security Procedures for Personal Computers distributed by your office. This publication is a great improvement over previous versions, and we recognize some of our earlier comments have been addressed. However, there are still some areas in which we have questions or concerns.

2. We believe that the next version of the publication would benefit from incorporating these changes. For further information on the attached comments, please contact [redacted] on STAT [redacted] If I can be of any assistance, please let me know.

STAT [redacted]

Attachment:
As Stated

ATTACHMENT

OIT Comments on
Security Procedures for Personal Computers

Overall, the Security Procedures for Personal Computers is a very worthwhile publication and is really needed by the user community. We realize that this publication intends to provide the minimum security procedures for all Agency components, but more specific detailed instructions would be helpful to the reader.

1. The document does not have a version number or a publication date on the front cover. Two versions have been published to date and there is no easy way for the customer to identify the more current version. The use of a light gray background with white lettering for the cover makes the title of the publication difficult to read. The use of a darker background color would make the title stand out as well as the document.

2. The publication never defines what is meant by "personal computer," so there is some uncertainty as to just what machines would fall under these procedures. For example, is the Xerox 1100 (Golden Tiger) a personal computer (PC)? What about a Delta Data terminal equipped with a disk drive, a Chromatics workstation on TADS, or a standalone minicomputer?

3. In those cases when security procedures call for an action to be "coordinated" with or approved by some specific component, it would be helpful if the reason for coordination and the conditions under which approval is granted or denied were supplied. For example, Section IV.D indicates that all product demonstrations by vendors must be coordinated with OS/ISSD. The reasons for this requirement should be made clear. Under what circumstances might OS/ISSD deny my request to have a vendor demonstrate a product? How does coordination take place? Does it require only a telephone call, or must a form be submitted or a memorandum be written? Does coordination imply approval? These same concerns apply in Sections IV.A (acquisition of PCs), VII (changing from one PC security configuration to another), VII.C.1 (removal of unclassified-outside PCs), VIII.F (requests for PC networks), IX.B (use of summer-only employees), IX.C (use of modems), IX.E (use of classified PCs that have been outside Agency control), and XI.B.3 (service representative access to non-sanitized PCs).

4. What is required to obtain a waiver from OS/ISSD (Section VI.B.1)? Why is an Agency Top Secret clearance required to have access to an unclassified PC? The publication makes no distinction between access to classified PCs and unclassified PCs.

5. In discussing physical security of PCs in an uncontrolled environment (Section VI.B.2), the publication states that access to all PCs must be controlled by an OS-approved access control device. The only example given is a Simplex lock. It is our understanding that a Simplex lock does not provide protection, since it is a trivial task to try all possible combinations of the lock in a short time (that is why visual contact with a vault door must be maintained at all times, even though there is a Simplex lock on the door). What other access control devices are there? Further, this section is supposed to be discussing security in an uncontrolled environment, yet seems to say that the first thing required is that the environment be controlled.

6. Section VI.B.2 also makes no distinction between classified and unclassified PCs when it requires that all media be removable, that all PCs must be turned off when unattended, and that the system be under the control of a TS-cleared person.

7. Section VI.B.3 discusses a security check sheet for each PC. This seems like a reasonable idea, but perhaps the idea should be extended to also apply to PC peripherals, such as printers and plotters. Peripherals should probably also be designated as classified or unclassified, with specific procedures for securing the classified devices.

8. The reason for a distinction between unclassified-inside and unclassified-outside use is not clear. If the systems are unclassified, why does it matter where they are used? Why is it not allowed to link the two types of machines (Section VII.C.2)? Is a PC located in an Agency facility designated unclassified-inside or -outside if it is used for accessing an external database? If a PC is designated as unclassified-outside, can it ever be operated inside an Agency facility?

9. Section VII.C.3 mentions a log that the System Administrator must keep. What information should be in the log? How long must the log be kept after the equipment is returned? Is there a standard format to be used, or is a stack of scraps of paper sufficient?

10. Similarly, Section VIII.D references an audit trail that must be kept for accesses to a local area network. What information should be audited? What format is acceptable? How long must the trail be maintained? How often should it be reviewed?

11. The limitations on PC network security in Section VIII apply only to non-mainframe networks. Why are mainframe networks exempt? Some of the restrictions imposed on PC networks are not currently enforced on our mainframe systems (items B, C, and E). Does item E really mean that an individual must be cleared for access to all information on the network in order

to use any portion of the information on the network? If that is true, then why does the server also have to enforce compartmentation of information (item C)?

12. Physically separating classified and unclassified PCs sounds like a fine idea. However, with existing space problems, requiring that an unclassified (or classified) PC have a room or cubicle all to itself is not realistic. We do not put classified safes in a separate room from unclassified file cabinets; why should we force such a strong distinction for PCs?

13. We suggest that Section X.B be clarified. It seems to state that in order to reuse media, it is necessary to sanitize the PC. Surely this is not the case. The reference to "unclassified inside PCs" is also unclear. Section X.C states that vendor software should never be returned to the vendor. We believe a stronger statement is necessary. The statement should indicate that magnetic media will never be returned to the vendor.

14. There are a few places in the publication where specific utilities are mentioned that can aid in PC security. Since these sections of the publication only apply to a small number of machine types, can it be assumed that the remainder of the publication also only applies to those same machine types? If not, then a distinction must be made throughout the document whenever the procedures does not apply to all PCs. For example, Section X.C.2 states that an individual must use the KOPY program (described later in Section XII) when writing unclassified data from a classified PC, yet the KOPY program is not available for all PCs. Further, it is not clear what products can be used with which machines. For example, the Wang PC runs DOS, so stating that a product works under DOS, and another version works on the Wang PC, would seem to imply that the DOS version in fact only works on some subset of PCs that run DOS.

15. Section X.E and Section X.F indicate that the System Administrator must receive and retain copies of the Form 4261 when used for recording the movement of magnetic media. The actions required of the System Administrator after receiving the forms should be spelled out.

16. Section X.G gives the responsibility for media classification and storage to the System Administrator; perhaps these are PC user responsibilities instead. Making the SA responsible is like having OIT responsible if AIM users inappropriately classify AIM documents, or if they leave a classified printout unsecured.

17. In Section XII, Consulting Services Branch of OIT should not be listed as a distributor of the PC security programs. We

have obtained the current version of these programs for our evaluation and until we can certify these programs as adequate for the protection of classified information, we cannot agree to distribute them. We are primarily concerned with the correctness of these programs and the integrity of the products produced by their use.

18. The example given in item 3 of the PC Security Guideline probably could be improved. It appears that perhaps the columns are not aligned, or the line length of the format is longer than the width of the page, so that the end of the line shows up on the next line. As a result, part of the serial number appears under the "Qty" heading. Further, all that appears under the "Item" heading is the brand name of the device (IBM). The item should probably be IBM PC, IBM Monitor, or IBM Printer. The Model should then be which specific PC version, monitor type, or printer type.

19. Item 10 of the PC Security Guideline refers to getting a PC approved by COMSEC. This is the only reference to COMSEC in the publication. Should COMSEC be another one of the offices listed in Section IV.A that must be coordinated with for acquisition of PCs?

20. The publication does not address "loaner" machines at all. These are machines that are not owned by the Agency, nor by employees, but are loaned by vendors to Agency components for evaluation,with the intention of returning the machines to the vendors after the evaluation period.

21. There are a few typesetting and typographical errors in the publication. The heading for Section VI is indented too far. In Section VII.A.1, the words "information every processed" should be changed to "information ever processed." There is an extra comma after "(DOS)" in Section X.H. In Section X.I, the words "turned into" should be changed to "turned in to." In Section XI.A, the word "anestablished" should be changed to "an established." The instructions for preparing a PC Security Plan state to use the underlined headings, but there are no headings underlined (they are italicized). In item 6 of the PC Security Guideline, the word "Usersand" should be changed to "Users and." Finally, the use of hyphens in "unclassified-inside" and "unclassified-outside" is inconsistent (sometimes there are no hyphens).

22. This publication does not adequately address PCs installed in the field, both domestic and foreign environments. We suggest producing a sterile version of this publication for use in the field.